

1 **IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

2 Serial No.
3 Filing Date Filed Concurrently Herewith
4 Inventorship Mironov
5 Applicant Microsoft Corporation
6 Attorney's Docket No. MS1-1921US
7 Title: Stream Cipher Design with Revolving Buffers

8 **INFORMATION DISCLOSURE STATEMENT**9 *References -- See Attached Form PTO-1449*10 **REMARKS**

11 The citations listed, copies of non- patent references attached, are submitted
12 in compliance with the duty of disclosure defined in 37 CFR §1.56. The Examiner
13 is requested to make these citations of official record in this application.

14 Respectfully Submitted,

15 Date: March 31, 2004

16 By: Ramin Aghevli
17 Ramin Aghevli
18 Reg. No. 43,462

EV 430703072 +

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U. S. Patent and Trademark Office, Washington, DC 20231. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO:** Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box → +

EV430703072 +

<p>Substitute for form 1449B/PTO</p> <p>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</p> <p><i>(use as many sheets as necessary)</i></p>				Complete if Known	
				Application Number	
				Filing Date	
				First Named Inventor	
				Group Art Unit	
				Examiner Name	
Sheet	2	of	2	Attorney Docket Number	MS1-1921US

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
		ALON, N., ROICHMAN, Y.; "Random Cayley Graphs and Expanders" RSA: Random Structures & Algorithms; January 7, 1997; 15 pgs	
		COURTOIS, N.; "Algebraic Attacks on Combiners with Memory and Several Outputs" Published on the internet at http://eprint.iacr.org/2003/125/ . Presented at Crypto 2003, 17 pgs	
		GOLIC, J. Dj.; "Cryptanalysis of Alleged A5 Stream Cipher" Springer-Verlag, 1998, pgs 239-255	
		HALEVI, S., COPPERSMITH, D., JUTLA, C.; "Scream: a software-efficient stream cipher" Published on the internet at http://eprint.iacr.org/2002/019.pdf . June 2002, pgs 1-21	
		ROGAWAY, P., COPPERSMITH, D.; "A Software-Optimized Encryption Algorithm" Journal of Cryptology: the journal of the International Association for Cryptologic Research, 1994, Revised Sept. 1997, 16 pgs	
		MENEZES, A., van OORSCHOT, P., VANSTONE, S.; "Handbook of Applied Cryptography" CRC Press, 1996 / 1997; Chapter 1 "Overview of Cryptography" pgs 1-48	
		MENEZES, A., van OORSCHOT, P., VANSTONE, S.; "Handbook of Applied Cryptography" CRC Press, 1996 / 1997; Chapter 6 "Stream Ciphers" pgs 191-222	

Examiner Signature		Date Considered	
-----------------------	--	--------------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Unique citation designation number. ² Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U. S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.